ON THE COMPUTATION OF HILBERT CLASS FIELDS

M. DABERKOW AND M. POHST

Abstract. Let k be an algebraic number field. We describe a procedure for computing the Hilbert class field $\Gamma(k)$ of k, i.e. the maximal abelian extension unramified at all places. In the first part of the paper we outline the underlying theory and in the second part we present the important algorithms and give several examples.

1. Preliminaries

The computation of Hilbert class fields has been an important issue in algebraic number theory in this century. After the connection between the j–function and the Hilbert class field for imaginary quadratic fields was established, various authors [ShiTa, Sta, Deu] improved and extended this analytic way of constructing (Hilbert) class fields. However, it is not yet clear whether this approach is suitable for arbitrary ground fields.

Following the precedence of Hasse [Ha], we describe a way of computing the Hilbert class field of an algebraic number field along the lines of the proof of the existence theorem of class field theory by Kummer extensions. This is a purely algebraic approach to the problem and can be used unconditionally. The algorithm outlined below has been implemented under the computer algebra system KASH [Kant].

In the sequel we consider an algebraic number field k and compute the maximal abelian extension $\Gamma(k)$ of k which is unramified at all places. This field $\Gamma(k)$ is called the Hilbert class field of k. Before we develop an algorithm for the computation of $\Gamma(k)$, we need to introduce some notation and state some theorems of the class field theory which are of importance for this work. We adopt the notation of [Janu]. We note, that in the special case of Hilbert class fields the conductor is always 1. A *subgroup* H of the group I_k of all fractional ideals of k always consists of the ideals of I_k which are contained in the ideal classes of a subgroup $\bar{H}$ of the class group Cl_k of k. In general, we make no distinction between $\bar{H}$ and H in the sequel.

In the subsequent section we use well-known results from the class field theory to reduce our task to the calculation of unramified relative extensions of prime degree. These are then computable as radical extensions if the ground field contains the appropriate roots of unity. In general, we must make a detour by firstly adjoining suitable roots of unity to our ground field k, then determining class fields over the obtained field, detecting the corresponding class fields over k and, eventually, forming composites of those. This procedure is lined out in section 3. In section 4 we discuss necessary refinements of the theory to make the approach computationally feasable. Section 5 contains several examples to demonstrate the potential of our method.

We note that real numbers are listed with 3 decimal digits (accuracy of 10^{-3}) in our examples.

The authors wish to thank H. Koch for various hints and comments which helped to improve this paper considerably.

2. Reduction

For determining the Hilbert class field $\Gamma(k)$ of an algebraic number field k we assume that the class group Cl_k of k is given as a direct product

$$Cl_k \;=\; H_1 \times \dots \times H_n$$

and that the order of H_i is the power of a prime number. We set

$$\tilde{H}_j \;:=\; H_1 \times \dots \times H_{j-1} \times H_{j+1} \times \dots \times H_n \quad (1 \le j \le n) \;.$$

Proposition 2.1. *If Γ_j denotes the class field of k corresponding to $\tilde{H}_j$ $(1 \le j \le n)$, then the Hilbert class field of k is the composite of $\Gamma_1, \dots, \Gamma_n$.*

This is an immediate consequence of the existence theorem of the class field theory. It reduces our task to the problem of determining class fields for subgroups H for which $Cl_k/\bar{H}$ is a cyclic group of prime power order. In the sequel we therefore assume that $\bar{H}$ is a subgroup of Cl_k fulfilling this condition.

The next Theorem will be used twofold,
(i) to break down the construction of a class field of prime power degree p^κ into κ steps of degree p each,
(ii) for a detour via Kummer extensions.
The latter is explained in detail in Section 3.

Theorem 2.2. *Let $\mathcal{F}/k$ be a cyclic extension, H be a subgroup of I_k and $H_{\mathcal{F}} := \{\mathfrak{a} \in I_{\mathcal{F}} \mid N_{\mathcal{F}/k}(\mathfrak{a}) \in H\}$. If $\mathcal{E}$ is the class field of $\mathcal{F}$ belonging to $H_{\mathcal{F}}$, then the class field Γ_H of k belonging to H is a subfield of $\mathcal{E}$ and the extension $\mathcal{E}/k$ is abelian. In this case the field $\mathcal{E}$ is the composite of $\mathcal{F}$ and Γ_H.*

This result follows immediately from the base change property of the Artin symbol.

Let us assume that G is a subgroup of Cl_k of index p^κ. Then there is an ascending chain of subgroups

$$G \;=\; G_s \;\subset\; G_{s-1} \;\subset\; \dots \;\subset\; G_0 \;=\; Cl_k$$

subject to $[G_i \,:\, G_{i-1}] \;=\; p \;\; (1 \le i \le s)$. The class fields belonging to the pair $(G_{s-i}\,, k)$ are denoted by Γ_i. Hence, we obtain a tower of field extensions

$$k \;=\; \Gamma_0 \;\subset\; \Gamma_1 \dots \;\subset\; \Gamma_s \;\;,$$

each step increasing the degree by a factor p.

Corollary 2.3. *The class field of Γ_i belonging to $N^{-1}_{\Gamma_i/\Gamma_0}(G_{s-i})$ is the class field of Γ_0 belonging to G_{s-i}.*

So far we simplified our problem to that of constructing class fields of prime degree p belonging to subgroups of the class group of index p. This will be discussed in the next section.

The two reductions of this section are illustrated with an example for which the results can be checked by other methods.

Example 2.4. *We consider the algebraic number field $k = \mathbb{Q}(\rho)$ with*

$$\rho^4 - 5\rho^2 + 196 = 0.$$

The following data were computed for k:

(1) *k is totally complex,*
(2) *an integral basis of k is given by:*

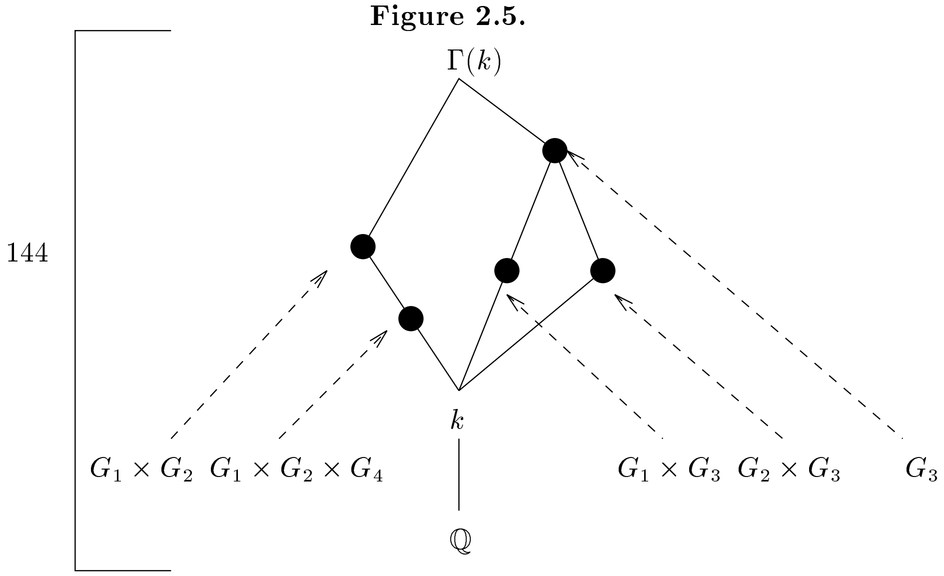
$$\begin{aligned} \mathcal{O}_k &= \mathbb{Z} + \rho\mathbb{Z} + \frac{1}{2}(\rho + \rho^2)\mathbb{Z} + \frac{1}{28}(14 + 9\rho + \rho^3)\mathbb{Z} \\ &=: \omega_1\mathbb{Z} + \omega_2\mathbb{Z} + \omega_3\mathbb{Z} + \omega_4\mathbb{Z}, \end{aligned}$$

(3) *the discriminant, regulator and class group of k are given by*

$$\begin{aligned} \mathfrak{d}_k &= 576081, \\ R_k &= 7.656, \\ Cl_k &\cong C_3 \times C_3 \times C_4 \\ &=: G_1 \times G_2 \times G_3. \end{aligned}$$

In order to compute the Hilbert class field $\Gamma(k)$of k, according to our reduction we have to compute the class fields of k belonging to $\tilde{G}_1 = G_2 \times G_3$, $\tilde{G}_2 = G_1 \times G_3$ and $\tilde{G}_3 = G_1 \times G_2$. The class fields belonging to $\tilde{G}_1$ and $\tilde{G}_2$ are of prime degree over k and therefore primitive over k. The class field Γ belonging to $\tilde{G}_3$ has Galois group isomorphic to C_4 and therefore a unique quadratic subfield Γ'. To compute Γ we will have to compute this class field first. If G_4 is the subgroup of order 2 of G_3, the class field Γ' belongs to the subgroup $G_1 \times G_2 \times G_4$ of Cl_k. Once Γ' is found, Γ will be computed as a class field to Γ' in a second step.

Figure 2.5.



We note that k is Galois of type V_4. This property is not used by our class group algorithm, but it can be used to obtain the class field in a different way. The three subfields of k are $k_1 := \mathbb{Q}(\sqrt{-23})$, $k_2 := \mathbb{Q}(\sqrt{-759})$, $k_3 := \mathbb{Q}(\sqrt{33})$. In our case the Hilbert class field $\Gamma(k)$ can already be obtained from k_1 and k_2. This will be done in Section 5.

3. Class fields of prime degree

Let p be a prime number dividing the class number h_k of k. In this section we develop a method for computing all subfields Γ of the Hilbert class field $\Gamma(k)$ of k with $[\Gamma : k] = p$. Each of these fields is the class field belonging to a subgroup G of Cl_k satisfying

$$|Cl_k \,/\, G| = p. \tag{3.1}$$

We denote the set of all these fields by Δ_p. Since we want to apply Kummer theory we need a base field which contains all p-th roots of unity. In case $p > 2$ this requires a detour via the extension $\mathcal{F} = k(\zeta_p)$, where ζ_p denotes a primitive p-th root of unity. From the class fields of $\mathcal{F}$ belonging to subgroups of index p in $CL_{\mathcal{F}}$ we obtain the corresponding class fields of k with Theorem 2.2.

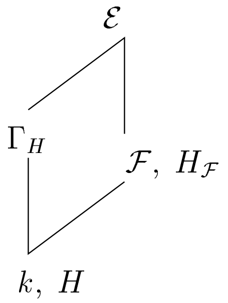


Figure 3.1.

For obvious reasons the cases $p = 2$ and $p > 2$ are treated separately in the sequel.

3.1. Case $p > 2$.
Let $\mathcal{F} = k(\zeta_p)$. In case ζ_p is not contained in k we can apply Theorem 2.2 to the cyclic extension $\mathcal{F}/k$.

Lemma 3.2. *The class field $\mathcal{E}$ of $\mathcal{F}$ belonging to $\mathrm{N}_{\mathcal{F}/k}^{-1}(H)$ is a Kummer extension of degree p, e.g. there is an $\eta \in \mathcal{K}$ with*

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\eta}) \quad .$$

This is a consequence of the properties of Kummer extensions and the degree of $\mathcal{F}$ over k being $p - 1$.

At this stage we have reduced the problem of the construction of Γ_H to the construction of a Kummer extension $\mathcal{E}$ and to the computation of a certain subfield of $\mathcal{E}$. We will deal with the problem of the computation of the subfield in a later section and concentrate now on the construction of $\mathcal{E}$.

The class field of $\mathcal{F}$ belonging to $\mathrm{N}_{\mathcal{F}/k}^{-1}(H)$ is a subfield of the Hilbert class field of $\mathcal{F}$ and therefore unramified at all places. Since $\mathcal{F}$ is a totally imaginary field, ramification can only occur at finite places and hence it is neccessary and sufficient for a finite abelian extension $\mathcal{E}$ having a relative discriminant equal to $o_{\mathcal{F}}$ to be a subfield of the Hilbert class field of $\mathcal{F}$. This is important for our construction, since there is an algorithm given in [Da] to compute the relative discriminant $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ of $\mathcal{E}/\mathcal{F}$ for a Kummer extension of prime degree. Since we did not use any specific information on H other than $|Cl_k/H| = p$, the idea outlined above applies to all subfields of the Hilbert class field of k with degree p over k, which were denoted by Δ_p.

Therefore the problem of computing Δ_p is reduced to the following three subproblems:

(1) the computation of all unramified abelian extensions $\mathcal{E}$ of $\mathcal{F}$ with $[\mathcal{E} : \mathcal{F}] = p$,

(2) the computation of all subfields $\mathcal{K}$ of each $\mathcal{E}$ such that $k \subset \mathcal{K}$, $\mathcal{K}/k$ is abelian and $[\mathcal{K} : k] = p$ holds,
(3) the validation of $\mathcal{K}$, e.g. proving that $\mathcal{K}$ is a subfield of the Hilbert class field of k.

To compute all unramified abelian extensions $\mathcal{E}$ of $\mathcal{F}$, we note the following theorem, which can be found in [He] (note that this theorem is true for all primes):

Theorem 3.3. *Let $\mathcal{E}$ be an algebraic number field with*

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$$

for a $\mu \in o_{\mathcal{F}}$. Then for $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ $\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}^p$, if $\gcd(\nu_{\mathfrak{p}}(\mu), p) = 1$. *In the case* $\gcd(\nu_{\mathfrak{p}}(\mu), p) = p$ *we have:*

(i) *For $\mathfrak{p} \nmid p$ we have $\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_p$ if the congruence $x^p \equiv \mu \mod \mathfrak{p}$ has a solution and $\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}$ if there is no solution to the congruence.*
(ii) *If $\mathfrak{p} | p$ holds, we have with $\mathfrak{e}_0 := \nu_{\mathfrak{p}}(p)/(p-1)$:*
   (a) *$\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_p$ if the congruence $x^p \equiv \mu \mod \mathfrak{p}^{\mathfrak{e}_0 p+1}$ has a solution,*
   (b) *$\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}$ if the congruence $x^p \equiv \mu \mod \mathfrak{p}^m$ is solvable for $m = \mathfrak{e}_0 p$, but not for $m = \mathfrak{e}_0 p + 1$.*
   (c) *$\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}^p$ if the congruence $x^p \equiv \mu \mod \mathfrak{p}^{\mathfrak{e}_0 p}$ has no solution.*

This theorem shows that the principal ideal $\mathfrak{a} = \mu o_{\mathcal{F}}$ must be the p–th power of an ideal in $o_{\mathcal{F}}$ if μ generates an unramified Kummer extension of degree p over $\mathcal{F}$. Hence, if $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu}) \neq \mathcal{F}$ is unramified over $\mathcal{F}$ for some $\mu \in o_{\mathcal{F}}$, we have $\mu o_{\mathcal{F}} = \mathfrak{a}^p$ for some ideal $\mathfrak{a} \subset o_{\mathcal{F}}$ and for the class A of $\mathfrak{a}$ in $Cl_{\mathcal{F}}$ we conclude $\mathrm{ord}_{Cl_{\mathcal{F}}}(A) \in \{1, p\}$. Since $\mathrm{ord}_{Cl_{\mathcal{F}}}(A) = 1$ would yield $[\mathcal{E} : \mathcal{F}] = 1$, we have $\mathrm{ord}_{Cl_{\mathcal{F}}}(A) = p$. We have just shown the next proposition.

Proposition 3.4. *Let $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_m\}$ be a (minimal) set of ideals satisfying*

$$\{\mathfrak{a}_1 \mathcal{P}_{\mathcal{F}}, \ldots, \mathfrak{a}_m \mathcal{P}_{\mathcal{F}}\} = \{A \in Cl_{\mathcal{F}} \mid \mathrm{ord}_{Cl_{\mathcal{F}}}(A) = p\},$$

and let $\alpha_1, \ldots, \alpha_m \in o_{\mathcal{F}}$ be fixed with $\alpha_i o_{\mathcal{F}} = \mathfrak{a}_i^p$ $(1 \le i \le r)$. Finally, let $\{\epsilon_1, \ldots, \epsilon_s\}$ be a set of representatives of the factor group $U_{\mathcal{F}}/U_{\mathcal{F}}^p$ of the unit group of $\mathcal{F}$.
If $\mathcal{E}$ is an unramified Kummer extension of degree p over $\mathcal{F}$, we have $\mathcal{E} = \mathcal{F}(\sqrt[p]{\epsilon_i \alpha_j})$ for some $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, r\}$.

As an application of this proposition we are now able to compute all unramified abelian extensions of $\mathcal{F}$ of degree p. To do so, let $\{G_1, \ldots, G_m\}$ be the set of all subgroups of the class group such that G_i is a cyclic group of order p and let $\mathfrak{a}_i$ be a representative of a generator of G_i $(1 \le i \le m)$. Finally, let α_i be a generator of the principal ideal $\mathfrak{a}_i^p$ $(1 \le i \le m)$ and let

$$U_{\mathcal{F}}^{(p)} = < \zeta_0 > \times < \zeta_1 > \times \ldots \times < \zeta_r >$$

be a subgroup of finite index I in $U_{\mathcal{F}}$ such that $p \nmid I$, where ζ_0 is a torsion unit of $\mathcal{F}$ and $\zeta_1, \dots, \zeta_r$ are independent units of $\mathcal{F}$. In the following we will call such a subgroup of $U_{\mathcal{F}}$ a p–maximal unit group. These ideals and algebraic numbers can be computed by methods outlined in [Po, PoZa, Co]. The set of all unramified abelian extensions of $\mathcal{F}$ of degree p is now a subset of

$$\Omega := \left\{ \mathcal{F}\left(\sqrt[p]{\zeta_0^{n_0} \cdot \dots \cdot \zeta_r^{n_r} \cdot \alpha_i^{n_{r+1}}}\right) \mid 1 \le i \le m,\ 0 \le n_j < p,\ 0 \le j \le r+1 \right\}$$

and can be computed by checking each extension $\mathcal{E} \in \Omega$ by computing the relative discriminant of $\mathcal{E}/\mathcal{F}$. This can be done by an algorithm given in [Da]. Note, that two generators $\sqrt[p]{\zeta_0^{n_0} \cdot \dots \cdot \zeta_r^{n_r} \cdot \alpha_i^{n_{r+1}}}$ and $\sqrt[p]{\zeta_0^{m_0} \cdot \dots \cdot \zeta_r^{m_r} \cdot \alpha_i^{m_{r+1}}}$ can generate the same extension. Therefore the size of Ω is given by $m\frac{p^{r+2}-1}{p-1}$, since the number of cyclic subgroups of order p of $\mathbb{F}_p^{r+2}$ is $\frac{p^{r+2}-1}{p-1}$.

Once we have computed all unramified extensions $\{\mathcal{E}_1, \dots, \mathcal{E}_n\}$ of $\mathcal{F}$ such that $\mathcal{E}_i/\mathcal{F}$ is abelian of degree p, we have to find a way to compute the class fields of k belonging to subgroups of the class group satisfying (3.1), which are the fields we are looking for, from the fields $\{\mathcal{E}_1, \dots, \mathcal{E}_n\}$. By Theorem 2.2, Lemma **??** and the fact that the class field of $\mathcal{F}$ belonging to $\mathrm{N}_{\mathcal{F}/k}^{-1}(H)$ is a subfield of the Hilbert class field of $\mathcal{F}$, we conclude by Galois theory that $\Gamma \in \Delta_p$ is a subfield of at least one field in $\{\mathcal{E}_1, \dots, \mathcal{E}_n\}$. A necessary condition for $\mathcal{E}_i$ to have one $\Gamma \in \Delta_p$ as a subfield was given in Theorem 2.2, namely the extension $\mathcal{E}_i/k$ has to be abelian. So before we check if one $\Gamma \in \Delta_p$ is contained in $\mathcal{E}_i$ for some i, we first check if the extension $\mathcal{E}_i/k$ is abelian. A necessary and sufficient condition for this fact is given in Shafarevich [Sha], though the result was certainly already known to Hilbert.

Lemma 3.5. *Let $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ be a Kummer extension of $\mathcal{F}$ and let σ be a generating automorphism of the Galois group $Gal(\mathcal{F}/k)$ such that $\sigma(\zeta_p) = \zeta_p^{\kappa}$. The extension $\mathcal{E}/k$ is abelian if and only if there is a $\mu_0 \in \mathcal{F}$ satisfying*

$$\sigma(\mu) = \mu_0^p \cdot \mu^{\kappa}.$$

This lemma enables us to test whether a given Kummer extension $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ over $\mathcal{F}$ is abelian over k or not by simply checking if $\sigma(\mu)/\mu^{\kappa}$ is a p-th power in $\mathcal{F}$. This can be done by either finding a linear factor of $t^p - \sigma(\mu)/\mu^{\kappa}$ in $\mathcal{F}[t]$ or by applying Montgomery's algorithm [Mo]. Moreover, we can easily compute the unique subfield $\tilde{\Gamma}$ of $\mathcal{E}$ with $[\tilde{\Gamma} : k] = p$, since this field is the fixed field of the k–automorphism ϕ of $\mathcal{E}$ defined by

$$\phi(\sqrt[p]{\mu}) = \mu_0 \sqrt[p]{\mu}^{\kappa}, \quad \phi(\zeta_p) = \zeta_p^{\kappa}$$

and can therefore be computed by linear algebra. So, without loss of generality, let $\{\mathcal{E}_1, \dots, \mathcal{E}_m\}$ $(m \le n)$ be the set of all $\mathcal{E}_i$ such that $\mathcal{E}_i/k$ is abelian (and hence cyclic) and let Γ_i be the (unique) subfield of $\mathcal{E}_i$ with $[\Gamma_i : k] = p$ $(1 \le i \le m)$. We define $\widetilde{\Delta_p}$ be the set of all these fields Γ_i.

It now remains to check for all $\Gamma \in \widetilde{\Delta_p}$ whether or not $\Gamma \in \Delta_p$ holds. We certainly know that each $\Gamma \in \widetilde{\Delta_p}$ is abelian over k, so it just remains to prove that Γ is unramified at all places over k. If the number of fields in $\widetilde{\Delta_p}$ equals the number of class fields of degree p (which certainly is known), we do not need to prove the correctness of the result. Otherwise we proceed as follows. Let $\Gamma \in \widetilde{\Delta_p}$ be a candidate for a class field belonging to Δ_p. By construction, Γ is given by a k–basis as a subfield of $\mathcal{E}_i$. Since this extension is primitive, there is a basis element of Γ such that the minimal polynomial of that element over k has degree p. Therefore it is easy to compute a primitive element of Γ over k [Tra, PoZa], hence over $\mathbb{Q}$, and we are able to compute the signature of Γ [PoSchDi], and therefore the ramification of the infinite primes. To verify that Γ is unramified over k at all finite primes, we compute the absolute discriminant $\mathfrak{d}_\Gamma$ of Γ. There is no ramification of Γ/k at finite primes if and only if $|\mathfrak{d}_k^p| = |\mathfrak{d}_\Gamma|$. As already mentioned, we need to know the discriminant of the potential class field Γ to prove that this field is one of the fields we are looking for. The field Γ can be given as an extension of k as well as a k-vector space in a Kummer extension $\mathcal{E}$ of degree p over $\mathcal{F}$. We will use the second representation to compute $\mathfrak{d}_\Gamma$.

By an algorithm given in [Da], an integral basis of $o_{\mathcal{E}}$ can easily be computed. So we can assume, that we know an integral basis $\eta_1, \dots, \eta_{[\mathcal{E}:\mathbb{Q}]}$ of $o_{\mathcal{E}}$. Since we know a k–basis of Γ in $\mathcal{E}$, we can compute a $\mathbb{Q}$ basis $\tau_1, \dots, \tau_{[\Gamma:\mathbb{Q}]}$ of Γ in $\mathcal{E}$. Then it is easy to compute an integral basis of $\mathcal{O}_\Gamma$ since we have $\mathcal{O}_\Gamma = \Gamma \cap o_{\mathcal{E}}$. This can be done by simple linear algebra. So let $\xi_1, \dots, \xi_{[\Gamma:\mathbb{Q}]} \in \mathcal{E}$ be an integral basis of Γ. Then we have

$$\mathfrak{d}_\Gamma = ([\mathcal{E} : \Gamma]^{[\Gamma:\mathbb{Q}]})^{-1} \det(\mathrm{Tr}_{\mathcal{E}/\mathbb{Q}}(\xi_i \xi_j)).$$

3.2. Case $p = 2$.

The case $p = 2$ can be treated quite similarly to the last one. We can leave out some of our arguments.

As in the previous section, we consider all Kummer extensions of $k(\zeta_2) = k$ unramified at all finite places. These extensions are not necessarily unramified at the infinite places as the example $\mathbb{Q}(\sqrt{-2}, \sqrt{6})/\mathbb{Q}(\sqrt{6})$ shows. By the method described for the case $p > 2$ we can compute all extensions $\mathcal{E}$ of k of degree 2 such that $\mathcal{E}/k$ is unramified at all finite places, e.g. has discriminant $\mathcal{O}_k$. One of these extensions has to have the appropriate ramification at the inifinite places, e.g the correct signature by Proposition 3.4. By computing a primitive element of each such field $\mathcal{E}$ over $\mathbb{Q}$ this can be checked easily.

4. Reduction of Ω

The stated algorithm has one major problem. This is the number of Kummer extensions that have to be considered during the computation. The set Ω tends to be very large for primes greater than 2, and we cannot give the precise size (or at least an upper bound) of Ω in terms of k, since this would require a precise knowledge of the p–rank of $Cl_{\mathcal{F}}$, where $\mathcal{F}$ is again $k(\zeta_p)$ and the p–rank of $Cl_{\mathcal{F}}$, denoted by $\mathrm{rank}_p(Cl_{\mathcal{F}})$, is the number of cyclic factors with order being a power of p in the complete decomposition of $Cl_{\mathcal{F}}$ in cyclic groups of prime power order. The only known results are related to Iwasawa theory and we have, for example, the following lower bound for $\mathrm{rank}_p(Cl_{\mathcal{F}})$ if k is totally real and p is odd [Wa, La90].

Theorem 4.1. *Let C^+ be the p–Sylow subgroup of the class group of k and C^- be the kernel of the norm map $N_{\mathcal{F}/k}(\cdot)$ from the p–Sylow subgroup of $Cl_{\mathcal{F}}$ onto Cl_k. Then we have $rank_p(C^+) \leq rank_p(C^-) + 1$ and therefore*

$$rank_p(Cl_{\mathcal{F}}) \geq 2 rank_p(C^+) - 1,$$

since we have $C = C^+ \oplus C^-$ for the p–Sylow subgroup of $Cl_{\mathcal{F}}$. If the extension $\mathcal{F}(\mu_{\mathcal{F}}^{1/p})$, where $\mu_{\mathcal{F}}$ is the group of roots of unity in $\mathcal{F}$, is ramified over $\mathcal{F}$, we have $rank_p(C^+) \leq rank_p(C^-)$, which implies

$$rank_p(C) \geq 2 rank_p(C^+).$$

Let r be the unit rank of $\mathcal{F}$ and r_p the p–rank of $Cl_{\mathcal{F}}$. Then the set Ω consists of $\frac{p^{r_p}-1}{p-1}p^{r+2}$ Kummer extensions. For each of these extensions we would have to test whether or not the extension is ramified at a finite place by computing the relative discriminant.

Example 4.2. *To compute the (unique) subfield Γ_3 with $[\Gamma_3 : k] = 9$ of the Hilbert class field of the field k given in Example 2.4, we would have to consider $\frac{3^2-1}{3-1}\frac{3^5-1}{3-1} =$ 484 Kummer extensions to compute all unramified extensions of $k(\zeta_3)$ since we have $Cl_{k(\zeta_3)} \cong C_2 \times C_3 \times C_3$. This would be still in a practical range, but to compute the Hilbert class field of $\mathbb{Q}(\rho)$, with $\rho^3 - 36\rho + 1 = 0$, which has class number 5, we would already have to consider*

$$\frac{5^2-1}{5-1}\frac{5^7-1}{5-1} = 117186$$

extensions since the class group of $\mathbb{Q}(\rho, \zeta_5)$ is isomorphic to $C_5 \times C_{170}$.

This example shows that it is crucial for the algorithm to reduce the size of Ω. We will give a sieving method to reduce the size of Ω during the computations. So we want to remove extensions from Ω by analyzing the results of already computed extensions.

Let G be a subgroup of $Cl_{\mathcal{F}}$ of order p generated by $\mathfrak{a}\mathcal{P}_{\mathcal{F}}$ and let α be a generator of the principal ideal $\mathfrak{a}^p$. Without loss of generality we assume,

$$p \notin \mathfrak{a}. \tag{4.1}$$

Furthermore let $U_{\mathcal{F}}^{(p)} =< \zeta_0 > \times < \zeta_1 > \times \ldots \times < \zeta_r >$ be a p–maximal unit group of $U_{\mathcal{F}}$. Then a subset of Ω is given by

$$\Omega_G = \left\{ \mathcal{F}\left(\sqrt[p]{\zeta_0^{n_0} \cdot \ldots \cdot \zeta_r^{n_r} \cdot \alpha^{n_{r+1}}} \right) \mid 0 \le n_j < p,\ 0 \le j \le r+1 \right\}.$$

As already mentioned, the set Ω_G contains $\frac{p^{r+2}-1}{p-1}$ extensions.

Our aim is to reduce the size of this set Ω_G successively. By Theorem 3.3 we can conclude that for a given $\mathcal{E} \in \Omega_G$ a prime ideal $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ can only be ramified in $\mathcal{E}/\mathcal{F}$ if $p \mid \mathfrak{p}$. As a consequence, to find the unramified extensions in Ω_G we only have to concentrate on ramification of prime ideals above p. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals above p in $\mathcal{F}$. The following proposition is an immediate consequence of Theorem 3.3.

Proposition 4.3. *Let $\mathcal{E}_i = \mathcal{F}(\sqrt[p]{\mu_i})$ $(i = 1, 2)$ be two extensions in Ω_G with relative discriminants $\mathfrak{d}_1$ and $\mathfrak{d}_2$ over $\mathcal{F}$ and $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu_1\mu_2}) \neq \mathcal{F}$. Then we have for $1 \le i \le n$*

$$\nu_{\mathfrak{p}_i}(\mathfrak{d}_1) \neq \nu_{\mathfrak{p}_i}(\mathfrak{d}_2) \Longrightarrow \nu_{\mathfrak{p}_i}(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}) > 0.$$

Thus if $\nu_{\mathfrak{p}_{i_0}}(\mathfrak{d}_1) \neq \nu_{\mathfrak{p}_{i_0}}(\mathfrak{d}_2)$ holds for some i_0, then $\mathcal{E}/\mathcal{F}$ is ramified.

Another sieving, which is a little bit more complicated, will be discussed in the sequel. It deals with the case that for two given extensions $\mathcal{E}_1, \mathcal{E}_2 \in \Omega_G$ with relative discriminants $\mathfrak{d}_1$ and $\mathfrak{d}_2$, we have $\nu_{\mathfrak{p}_i}(\mathfrak{d}_1) = \nu_{\mathfrak{p}_i}(\mathfrak{d}_2)$ for some $i \in \{1, \ldots, n\}$. We make use of the following preparatory lemma [Da].

Lemma 4.4. *Let $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu}) \in \Omega_G$ be a Kummer extension of $\mathcal{F}$ ramified at $\mathfrak{p}_{i_0}$, e.g. $\nu_{\mathfrak{p}_{i_0}}(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}) > 0$ for some $i_0 \in \{1, \ldots, n\}$. With $\mathfrak{e}_0 := \nu_{\mathfrak{p}_{i_0}}(p)\frac{1}{p-1}$ and*

$$\kappa = \max\{0 \le k < \mathfrak{e}_0 p \mid \exists \gamma \in o_{\mathcal{F}} : \gamma^p \equiv \mu \mod \mathfrak{p}_{i_0}^k\},$$

we have $\gcd(\kappa, p) = 1$ and

$$\nu_{\mathfrak{p}_{i_0}}(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}) = (p-1)(\mathfrak{e}_0 p - \kappa + 1).$$

Proposition 4.5. *Let $\mathfrak{p}$ be a prime ideal contained in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and define $\mathfrak{e}_0 := \nu_{\mathfrak{p}}(p)\frac{1}{p-1}$. For $x, y \in o_{\mathcal{F}} \setminus \mathfrak{p}$, $\kappa := \lceil \frac{n}{p} \rceil$ and $n < \mathfrak{e}_0 p$ we have*

$$x^p \equiv y^p \mod \mathfrak{p}^n \Longleftrightarrow x \equiv y \mod \mathfrak{p}^\kappa.$$

Proof. "$\Longleftarrow$": By assumption we have $x \equiv y \mod \mathfrak{p}^\kappa$. Hence there is an $\alpha \in \mathfrak{p}^\kappa$ satisfying $x = y + \alpha$ and therefore we have

$$x^p \equiv (y+\alpha)^p \equiv y^p + \sum_{i=1}^{p-1} \binom{p}{i} y^{p-i}\alpha^i + \alpha^p \mod \mathfrak{p}^n.$$

From $\nu_{\mathfrak{p}}(y) = 0$ and $\nu_{\mathfrak{p}}(\alpha) \neq 0$ we conclude

$$\nu_{\mathfrak{p}}\left(\binom{p}{i} y^{p-i}\alpha^i\right) \neq \nu_{\mathfrak{p}}\left(\binom{p}{j} y^{p-j}\alpha^j\right)$$

for $1 \leq i < j \leq p-1$. Since we have $n < \mathfrak{e}_0 p$, it follows $\lceil \frac{n}{p} \rceil \geq n - \mathfrak{e}_0(p-1)$ and we get

$$\nu_{\mathfrak{p}}\left(\sum_{i=1}^{p-1}\binom{p}{i} y^{p-i}\alpha^i\right) = \nu_{\mathfrak{p}}(p) + \nu_{\mathfrak{p}}(\alpha) \geq \mathfrak{e}_0(p-1) + n - \mathfrak{e}_0(p-1) = n.$$

Moreover, we have $\nu_{\mathfrak{p}}(\alpha^p) = p\nu_{\mathfrak{p}}(\alpha) \geq p\lceil \frac{n}{p} \rceil \geq n$ and the assertion is proved .

"$\Longrightarrow$": Assume $x = y + \alpha$ with $\alpha \notin \mathfrak{p}^\kappa$. Then we have $\nu_{\mathfrak{p}}(\alpha) \leq \kappa - 1$, $\nu_{\mathfrak{p}}(\alpha) < \mathfrak{e}_0$ and

$$p\nu_{\mathfrak{p}}(\alpha) \leq p(\kappa - 1) < p\left(\frac{n}{p} + 1\right) - p = n + p - p = n,$$

where the second inequality follows from

$$\nu_{\mathfrak{p}}(\alpha) \geq \mathfrak{e}_0 \Rightarrow \kappa > \mathfrak{e}_0 \Rightarrow n > \mathfrak{e}_0 p,$$

which is a contradiction to $n < \mathfrak{e}_0 p$. Now let r be $\sum_{i=1}^{p-1}\binom{p}{i} y^{p-i}\alpha^i$.
If n is less than $\nu_{\mathfrak{p}}(p)$, we have $\nu_{\mathfrak{p}}(r) \geq \nu_{\mathfrak{p}}(p) > n$ and therefore

$$x^p \equiv (y+\alpha)^p \equiv y^p + \alpha^p \not\equiv y^p \mod \mathfrak{p}^n.$$

In the case $n \geq \nu_{\mathfrak{p}}(p)$, we have $\nu_{\mathfrak{p}}(r) = (p-1)\mathfrak{e}_0 + \nu_{\mathfrak{p}}(\alpha) > p\nu_{\mathfrak{p}}(\alpha)$ and hence

$$\nu_{\mathfrak{p}}(r + \alpha^p) = \min\{(p-1)\mathfrak{e}_0 + \nu_{\mathfrak{p}}(\alpha),\ p\nu_{\mathfrak{p}}(\alpha)\} = p\nu_{\mathfrak{p}}(\alpha) < n.$$

So we proved $x^p \not\equiv y^p \mod \mathfrak{p}^n$, which is a contradiction to our assumption. Hence, we have $x \equiv y \mod \mathfrak{p}^\kappa$. □

Proposition 4.6. *Let $\mathcal{E}_i = \mathcal{F}(\sqrt[p]{\mu_i})$ $(i = 1, 2)$ be two extensions in Ω_G with relative discriminants $\mathfrak{d}_1, \mathfrak{d}_2$ over $\mathcal{F}$ such that there is an i_0 satisfying $\nu_{\mathfrak{p}_{i_0}}(\mathfrak{d}_1) = \nu_{\mathfrak{p}_{i_0}}(\mathfrak{d}_2) > 0$ and let $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu_1\mu_2}) \neq \mathcal{F}$. Defining $\mathfrak{e}_0 = \nu_{\mathfrak{p}_{i_0}}(p)\,\frac{1}{p-1}$ and*

$$n_i = \max\{0 \leq k \leq \mathfrak{e}_0 p + 1 \mid \exists\, \gamma \in o_{\mathcal{F}} : \gamma^p \equiv \mu_i \mod \mathfrak{p}_{i_0}^k\} < \mathfrak{e}_0 p \ \ (i = 1, 2),$$

we have $n_1 = n_2 =: n$. Let $\gamma_1, \gamma_2, \tilde{\mu_1}, \tilde{\mu_2}$ in $o_{\mathcal{F}}$ be given with $\gamma_i^p \equiv \mu_i \mod \mathfrak{p}_{i_0}^n$ and $\gamma_i^p + \tilde{\mu_i} \equiv \mu_i \mod \mathfrak{p}_{i_0}^{n+1}$. Then we have

$$\nu_{\mathfrak{p}_{i_0}}(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}) < \nu_{\mathfrak{p}_{i_0}}(\mathfrak{d}_1)$$

if and only if $(\gamma_1^p\tilde{\mu_2} + \gamma_2^p\tilde{\mu_1}) \equiv 0 \mod \mathfrak{p}_{i_0}^{n+1}$.

Proof. "$\Longleftarrow$": Obvious.
"$\Longrightarrow$": By Theorem 4.4 there must be a $\xi \in o_{\mathcal{F}}$ such that $\xi^p \equiv \mu_1\mu_2 \mod \mathfrak{p}^{n+1}$ holds. Hence, we have $\xi^p \equiv (\gamma_1\gamma_2)^p \mod \mathfrak{p}^n$ and

$$(4.2)\quad \xi^p \equiv (\gamma_1\gamma_2)^p + \tilde{\mu_1}\gamma_2^p + \tilde{\mu_2}\gamma_1^p + \tilde{\mu_1}\tilde{\mu_2} \equiv (\gamma_1\gamma_2)^p + \tilde{\mu_1}\gamma_2^p + \tilde{\mu_2}\gamma_1^p \mod \mathfrak{p}^{n+1}.$$

By the last proposition we conclude $\xi \equiv \gamma_1\gamma_2 \mod \mathfrak{p}^{\lceil \frac{n}{p} \rceil}$ and therefore there is an $\tilde{\xi} \in \mathfrak{p}^{\lceil \frac{n}{p} \rceil}$ such that $\xi = \gamma_1\gamma_2 + \tilde{\xi}$ holds. So with $r := \sum_{i=1}^{p-1} \binom{p}{i} (\gamma_1\gamma_2)^{p-i}\tilde{\xi}^i$ we have the congruence

$$\xi^p \equiv (\gamma_1\gamma_2)^p + r + \tilde{\xi}^p \mod \mathfrak{p}^{n+1}. \tag{4.3}$$

We will now prove $r \equiv \tilde{\xi}^p \equiv 0 \mod \mathfrak{p}^{n+1}$, with which we begin by showing $r \equiv 0 \mod \mathfrak{p}^{n+1}$. By Lemma 4.4 we have $\gcd(n,p) = 1$ and hence

$$\left\lceil \frac{n}{p} \right\rceil = \left\lceil \frac{n+1}{p} \right\rceil. \tag{4.4}$$

We have $x \leq \mathfrak{e}_0(p-1) + \frac{x}{p} \Leftrightarrow x \leq e_0 p$ for all $x \in \mathbb{R}$ and since $n+1 \leq \mathfrak{e}_0 p$ holds,

$$\begin{array}{rrl} & \mathfrak{e}_0(p-1) + \frac{n+1}{p} \geq & n+1 \\ \Longrightarrow & \mathfrak{e}_0(p-1) + \lceil \frac{n+1}{p} \rceil \geq & n+1 \\ \Longrightarrow & \mathfrak{e}_0(p-1) + \lceil \frac{n}{p} \rceil \geq & n+1. \end{array}$$

follows from (4.4). So $r \equiv 0 \mod \mathfrak{p}^{n+1}$ is now a consequence of $\nu_{\mathfrak{p}}(r) = \mathfrak{e}_0(p-1) + \nu_{\mathfrak{p}}\left(\tilde{\xi}\right) \geq \mathfrak{e}_0(p-1) + \lceil \frac{n}{p} \rceil \geq n+1$. It remains to prove that $\tilde{\xi}^p \equiv 0 \mod \mathfrak{p}^{n+1}$ holds, too.

By the definition of $\tilde{\xi}$ we have $\tilde{\xi}^p \equiv 0 \mod \mathfrak{p}^n$ and by (4.4) we have

$$p\left\lceil \frac{n}{p} \right\rceil = p\left\lceil \frac{n+1}{p} \right\rceil \geq p\frac{n+1}{p} = n+1,$$

and therefore $\nu_{\mathfrak{p}}\left(\tilde{\xi}^p\right) \geq n+1$, so that $\tilde{\xi}^p \equiv 0 \mod \mathfrak{p}^{n+1}$ holds. The assumption follows now from (4.2) and (4.3). $\square$

5. Examples

We illustrate this discussion of the construction of Hilbert class fields with several examples.

Clearly, we start with Hasse's examples from [Ha]. The class field of $k = \mathbb{Q}(\sqrt{-31})$ of class number 3 is given by a root of the relative polynomial

$$x^3 + \frac{3+\sqrt{-31}}{2}x^2 + \frac{-3+\sqrt{-31}}{2}x - 1 \quad .$$

From a theoretical point of view the generation of $\Gamma(k)$ over $\mathbb{Q}$ by $\sqrt{-31}$ and a root ρ of the polynomial x^3+x+1 (of discriminant -31) is certainly preferable. However, we chose to list a relative polynomial since a root of it generates an order of $\Gamma(k)$ of smaller index than $\mathbb{Z}[\sqrt{-31}\,,\,\rho]$.

The class field of $k = \mathbb{Q}(\sqrt{-47})$ of class number 5 is generated by a root of the relative polynomial

$$x^5 + \frac{9-\sqrt{-47}}{2}x^4 + \frac{5-2\sqrt{-47}}{2}x^3 - \frac{5+3\sqrt{-47}}{2}x^2 - \frac{25+3\sqrt{-47}}{2}x - 5 \ .$$

As in the previous example we can generate $\Gamma(k)$ over $\mathbb{Q}$ by $\sqrt{-47}$ and a root ρ of the polynomial $x^5 + 3x^2 + 2x - 1$.

Both examples are computed on a medium fast work station in less than a minute.

The next example was already considered by Stark [Sta]. Stark computed the Hilbert class field of the totally real cubic field of smallest discriminant with class number 3 by using transcendental functions. The cubic field is generated by a root ρ of the polynomial $t^3 - t^2 - 9t + 8$. The invariants of k are:

(1) k is totally real,
(2) the discriminant, regulator and class group of k are given by

$$\mathfrak{d}_k = 2597, \quad R_k = 4.795, \quad Cl_k \cong C_3$$

and an integral basis of k is given by

$$\mathcal{O}_k = \mathbb{Z} + \rho\mathbb{Z} + \rho^2\mathbb{Z}.$$

A generating polynomial of $\Gamma(k)$ over k is

$$t^3 - (223 - 549\rho + 336\rho^2)t - 6229 + 12156\rho - 5766\rho^2,$$

and a generating polynomial over $\mathbb{Q}$ is

$$t^9 - 4t^8 - 3t^7 + 29t^6 - 26t^5 - 24t^4 + 34t^3 - 2t^2 - 5t + 1.$$

It took 13 seconds to compute this data for $\Gamma(k)$ on a HP 735 with 196 MB RAM. We note that the class number of $\Gamma(k)$ is one.

The second but last example is the field $k = \mathbb{Q}(\rho)$ with $\rho^4 - 5\rho^2 + 196$. The invariants of k were already given in Example 2.4. Figure 5.1 shows the relevant subfield lattice that occurs during the computations. The class group of $\mathcal{F} = k(\zeta_3)$ is isomorphic to $C_3 \times C_3 \times C_2$.

The result is $\Gamma(k) = k(\alpha\,,\,\beta)$ with

- α a root of

$$\begin{gathered}x^9+(-9+6\omega_4)x^8-(119+12\omega_2+19\omega_4)x^7\\+(902+82\omega_2-58\omega_3-380\omega_4)x^6\\+(3013+798\omega_2+213\omega_3+581\omega_4)x^5\\-(19168+3580\omega_2-1453\omega_3-7746\omega_4)x^4\\-(1702+2174\omega_2+5785\omega_3+12224\omega_4)x^3\\+(74948+31710\omega_2+5013\omega_3-21554\omega_4)x^2\\-(126690+47540\omega_2-10700\omega_3-51805\omega_4)x\\+(48475+9550\omega_2-10150\omega_3-19600\omega_4),\end{gathered}$$

- β a root of

$$\begin{gathered}x^4+(714+192\omega_2-192\omega_4)x^2-\\(72-144\omega_4)x+(909-704\omega_2+704\omega_4).\end{gathered}$$

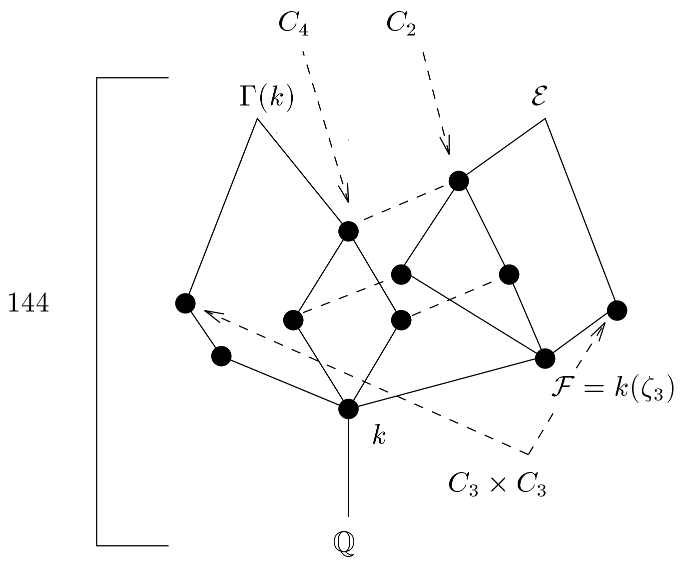


Figure 5.1.

The computation of $\Gamma(k)$ took 2 minutes on a HP 735 with 196 MB RAM. A generating polynomial of $\Gamma(k)$ over $\mathbb{Q}$ is omitted since the output would require several pages.

An alternative approach via the imaginary subfields of k yields $\Gamma(k)$ as follows. The field $k_1=\mathbb{Q}(\sqrt{-23})$ has class number 3. Its Hilbert class field $\Gamma(k_1)$ is therefore generated over $\mathbb{Q}$ by $\sqrt{-23}$ and a root ρ_1 of the polynomial x^3-x+1 (of discriminant -23). The field $k_2=\mathbb{Q}(\sqrt{-759})$ has class group $C_2\times C_{12}$. Its Hilbert class field $\Gamma(k_2)$ can easily be computed by analytic methods. Then a computation of the subfields of $\Gamma(k_2)$ yields the following generators over $\mathbb{Q}$:

$$\sqrt{33}\ ,\ \text{ a root } \rho_2 \text{ of } x^3 - x^2 + 6x - 3 \ \text{(of discriminant -759)}\ ,$$
$$\text{and a root } \rho_3 \text{ of } x^4 + 2x^3 + 2x^2 + x - 17\ .$$

Hence, we also find $\Gamma(k) \cong k(\rho_1, \rho_2, \rho_3)$. Those computations as well as the construction of an isomorphism are easily performed with KASH [Kant]. (A generation of $\Gamma(k)$ over $\mathbb{Q}$ can also be found from $k(\alpha\,,\,\beta)$ by a computation of the corresponding lattice of subfields.)

The final example is chosen in a way that all other presently known methods would fail.

We compute the class field of $k = \mathbb{Q}(\rho)$ for a root ρ of $x^3 + 28x + 175$. Clearly, k has one real and two complex conjugates. The discriminant of k is -914683 (k has a power integral basis), the regulator of k is 4.328, and the class group of k has the structure $C_6 \times C_{12}$. Hence, the class field $\Gamma(k)$ of k is of total degree 216 over $\mathbb{Q}$. We compute $\Gamma(k) = \mathbb{Q}(\tau_1, \tau_2, \tau_3, \tau_4)$, where the τ_i are zeros of the following polynomials $f_i(x)$ $(1 \le i \le 4)$:

$$f_1(x) \ := \ x^3 + x^2 - 2x - 1 \ \ (\tau_1 = 2\cos(2\pi/7))\ ,$$
$$f_2(x) \ := \ x^3 + \rho x^2 - 6x + 27\ ,$$
$$f_3(x) \ := \ x^2 - \rho x - (\rho + 2)\ ,$$
$$f_4(x) \ := \ x^4 - \rho x^3 - 22x^2 - (\rho^2 - 19\rho + 38)x - (3\rho^2 - 16\rho + 53)\ .$$

We note that $f_2(x)\,,\, f_3(x)\ ,\, f_4(x)$ cannot be substituted by polynomials in $\mathbb{Q}[x]$. The total computation time was a little less than 5 minutes in this case.

The whole algorithm for the computation of Hilbert class fields is implemented in KASH [Kant], which is public domain and can be obtained from

ftp.math.tu-berlin.de:/pub/algebra/Kant/Kash.

References

[Co] H. Cohen, *A Course in Computational Algebraic Number Theory*, 1. Aufl., Springer Verlag 1993.

[Da] M. Daberkow, *Computations in Kummer extensions I, II*, to appear.

[DaPo] M. Daberkow and M. Pohst, *Computations with relative extensions of number fields with an application to the construction of Hilbert class fields*; ISSAC'95 Proc.

[Deu] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Teubner Verlag, Stuttgart.

[FiPo] U. Fincke and M. Pohst, *A procedure for determining algebraic integers of given norm*, Proc. Eurosam 83, Springer Lecture Notes in Computer Science **162** (1983), 194 – 202.

[Ha] H. Hasse, *Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante* -47, Acta Arith. **9**, 419 – 434.

[He] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer Verlag 1981.

[Janu] G. J. Janusz, *Algebraic Number Fields*, sec. ed., Grad. Stud. in Math. vol. 7, Amer. Math. Soc. 1996.

[Kant] Kant group, KANT V4, to appear in Journal of Symbolic Computations.

[La86] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics 110, Springer Verlag 1986.

[La90] S. Lang, *Cyclotomic fields I and II. Combined 2nd ed.*, Graduate Texts in Mathematics 121, Springer Verlag 1990.

[Mo] P.L. Montgomery, *Square roots of products of algebraic numbers*, Proceedings of Symposia in Applied Mathematics, Vol. **48** (1994), 567 – 571.

[Ne] J. Neukirch, *Algebraische Zahlentheorie*, 1. Aufl., Springer Verlag 1992.

[Po] M. Pohst, *Computational algebraic number theory*, DMV Seminar Bd. 21, Birkhäuser Verlag 1993.

[PoSchDi] M. Pohst, A. Schwarz and F. Diaz y Diaz, *A Table of Quintic Fields*, Math. Comp. **63** (1994), 361–376.

[PoZa] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press 1989.

[Sha] I.R. Shafarevich, *A new proof of the Kronecker Weber theorem*, Shafarevich, Collected Mathematical Papers, Springer Verlag 1989.

[ShiTa] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan No. **6** 1961, Tokyo.

[Sta] H.M. Stark,*L–functions at* $s = 1$. *IV. First derivatives as* $s = 0$., Adv. Math. **35**, 197–235.

[Tra] B. M. Trager, *Algebraic Factoring and Rational Function Integration*, Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation (SYMSAC 76), 219 – 226.

[Wa] L. Washington, *Introduction to cyclotomic fields.* Graduate Texts in Mathematics 83, Springer Verlag 1982.